# **Exhibit 2 –**
# Declaration of
# Matthew Schruers (CCIA)

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF TEXAS**
**AUSTIN DIVISION**

| | | |
|---|---|---|
| COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, and<br><br>NETCHOICE, LLC,<br><br>*Plaintiffs*,<br><br>v.<br><br>KEN PAXTON, in his official capacity as Attorney General of Texas,<br><br>*Defendant*. | ) | Civil Action No. 1:24-cv-849 |

**DECLARATION OF MATTHEW SCHRUERS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION**

I, Matthew Schruers, declare as follows:

1. I am the President & CEO of the Computer & Communications Industry Association (CCIA). I have worked at the organization for nearly nineteen years. Upon joining the Association, I focused on legal, legislative, and policy matters, later taking on the roles of Chief Operating Officer and President. In each of these capacities, I have worked closely and communicated often with CCIA members regarding how public policy proposals affect their businesses, operations, and relationships with their users. Through my experience, I have also gained familiarity with how such proposals affect all manner of websites, applications, and other digital services.[1]

2. I submit this declaration in support of Plaintiffs' Motion for Preliminary Injunction. I am over the age of 18 and am competent to make the statements herein. I have personal

[1] This Declaration will refer to all digital services—including social media websites and applications—as "websites" unless necessary to distinguish among different kinds of digital services.

knowledge of the facts set forth in this declaration and, if called and sworn as a witness, could and would competently testify to them.

## I. About CCIA and CCIA's Affected Members

3. CCIA is an international, not-for-profit membership association representing a broad cross-section of companies in the computer, Internet, information technology, and telecommunications industries. For more than fifty years, CCIA has promoted open markets, open systems, and open networks, and advocated for the interests of the world's leading providers of technology products and services before governments and the courts.[2]

4. CCIA's membership includes computer and communications companies, equipment manufacturers, software developers, service providers, communications resellers, integrators, and financial service companies.[3] A number of CCIA's members would be considered "digital service providers" under Texas House Bill 18 (HB18) including, at a minimum: (1) Google, which owns and operates YouTube; (2) Meta, which owns and operates Facebook and Instagram; (3) Pinterest; and (4) X (formerly known as Twitter). These HB18-covered members enable billions of users around the world to create and share content using their services, whether to facilitate work, study, prayer, socialization, commerce, or communications. These companies also moderate and curate what is displayed on their services as a vital part of their operations. They disseminate a massive and constantly expanding amount of content in order to provide valuable products and tools for their users.

[2] CCIA, Home, https://perma.cc/T9EQ-5GC3.

[3] Currently, CCIA's members include: Amazon, Apple, Cloudflare, Coupang, Deliveroo, Dish Network, eBay, Google, Intel, Intuit, Meta, Nord Security, Opera, Pinterest, Rakuten, Red Hat, Shopify, Texas.net, TSMC, Uber, Viagogo, Waymo, X, and Zebra. *See* CCIA, Members, https://perma.cc/4CDL-UQAS.

5. Because content moderation is central to the operations of these CCIA members, issues surrounding trust and safety constitute a significant part of CCIA's policy and advocacy work. To that end—among our other endeavors and projects in this area—CCIA is incubating a non-profit organization called the Digital Trust & Safety Partnership (DTSP). DTSP partners include CCIA members and other businesses dedicated to improving practices and procedures for identifying and preventing the dissemination of objectionable and harmful content online. DTSP aims to develop and iterate upon industry best practices for, among other things, the moderation of third-party content and behavior, with the goal of ensuring a safer and more trustworthy Internet. DTSP's objectives include the facilitation of internal assessments—and, subsequently, independent third-party assessments—of participants' implementation of identified best practices for promoting the safety of their users and the online communities that they maintain. The organization balances these collective goals with the recognition that each of its participating companies has its own values, service aims, digital tools, and human-led processes for moderating the extremely broad range of human expression they facilitate.

## II. Valuable and Protected Speech on CCIA Members' Websites

6. The content on CCIA members' websites comes from all over the world and is incredibly diverse. The services enable and provide a forum for the height of human thought and creativity: material that runs the gamut from being culturally significant, informative, educational, or politically engaging to funny and entertaining. These services offer central avenues for protected speech and expression, and millions of individuals use these services daily to engage in speech.

7. CCIA members' websites offer access to a wide array of highly valuable speech and viewpoints, and adults and minors alike benefit from access to these websites. Many adults use at least one of CCIA members' websites, and so do "95% of teens." Emily A. Vogels, et al.,

*Teens, Social Media and Technology 2022*, Pew Research Center (Aug. 10, 2022), https://perma.cc/B226-6SKV. Even as of five years ago, three quarters of teens "report[ed] having at least one active social media profile, and 51% report[ed] visiting a social media site at least daily." *Social Media and Teens*, American Academy of Child & Adolescent Psychiatry (Mar. 2018), https://perma.cc/6DH5-GHV3. Accordingly, CCIA's members offer their users the opportunity to (1) maintain connections with friends and family and create new connections; (2) express themselves and their creative works; (3) stay informed about current events and engage in their own political and social speech on the day's issues; (4) learn from others, whether through expressly educational content or through the ability for cross-cultural exchange; and (5) simply find high-quality and engaging expression.

## III. The Need for Content Moderation

8. Content moderation – which includes the practices and systems used by digital services to manage and mitigate content- and behavior-related risks to users and others – serves a vital function in allowing websites to express themselves and effectuate their community standards, thereby delivering on commitments that they have made to their communities. Content rules and enforcement actions reflect normative judgments about what will best foster the kind of environment that companies have promised to their users.

9. Beyond their commitments to their communities, CCIA's covered members have every business incentive to address objectionable and harmful content and behavior on their websites. Rightly or not, members of the public often associate websites with the third-party content that appears on their services. Site users also associate brands that advertise on websites with content that appears on the websites. As a result, brand owners worry about the effects of such content on their brands that come from their brands being visible next to objectionable and

harmful content on websites. The reputational costs of such connections can be permanent. Research demonstrates that consumer sentiment toward social media services and their advertisers declines when those services do not respond to objectionable and harmful content. Melissa Pittaoulis, *Hate Speech & Digital Ads: The Impact of Harmful Content on Brands*, CCIA (Sept. 5, 2023), https://perma.cc/Q2PR-7A5Q. Failing to manage objectionable and harmful content causes significant harm to the business prospects of a digital service and its advertisers, jeopardizing a $3.7 trillion industry. Accordingly, organizations like DTSP have been at the forefront of creating and sharing best practices to guide digital service providers to a mature state of development for identifying and managing objectionable and harmful content online. DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* 1-9 (July 2022), https://perma.cc/Q2PR-7A5Q. Those best practices recognize, however, that "[t]here is no one-size-fits all solution" for these issues. DTSP, *Age Assurance: Guiding Principles & Best Practices* 2 (Sept. 2023), https://perma.cc/2SXF-BWQB.

10. In light of these imperatives, CCIA's covered members have developed numerous means of moderating objectionable and harmful content and behavior and are adept at catching objectionable and harmful content before the vast majority of users (if any) even see the content. Many CCIA members rely on a mix of technological tools and global teams of human reviewers to flag and address content. Additionally, these websites are constantly innovating ways to catch dangerous and/or illegal content through innovative means like machine-learning technology—and they work to share these innovations with other key stakeholders.

## IV. Content Moderation Hurdles

11. Achieving 100% accurate content moderation at the scale and scope CCIA members operate is not feasible. Even if a website has a 99.9% accuracy rate at addressing violative

content (meaning content that violates the website's terms and conditions of service), when potentially hundreds of millions of pieces of content are uploaded every day, violative content will still slip through. Many digital service providers rely heavily on automated systems to supplement their ability to address violative content before it is even seen. But content moderation has tradeoffs. Too much reliance on automated systems may be overinclusive and hamper users' experiences and access to valuable speech. Too little content moderation, however, will likely drive users and advertisers away. Thus, CCIA's members work hard to innovate ever-better trust and safety practices to find the proper balance. Yet various factors combine to make it so that objectionable or harmful content will evade their content moderation.

12. **Variety of Forms of Content.** Many CCIA members publish, disseminate, and display a wide variety of user-created online content in myriad forms—including human-readable text, source code and object code, videos, audio clips, and photographs. Each of these forms raises distinct content-moderation requirements and difficulties. Some content-moderation tools will work better for some forms of content and worse for others.

13. **Scale of Content and Kinds of Harmful Content.** The volume of content that these websites are called upon to moderate is staggering. The vast majority of this content is culturally significant, highly informative, brilliantly funny, or satirical. But a relatively small sliver of the vast amount of user-generated content is the opposite. Because almost anyone can create an account and post content on certain social media services, users can attempt to submit content ranging from dangerous, illegal, and abusive, to things that are just undesirable and annoying. The objectionable and harmful content that websites moderate varies greatly. It ranges from patently illegal content like child sexual abuse material (CSAM) as understood under U.S. federal law—which members remove and report to the National Center for Missing and Exploited Children

(NCMEC)—to hate speech and graphic violence. CCIA members expend great effort to make millions of different decisions every day about what content to moderate on their site. For instance:

a. Facebook and Instagram have over three billion users, and billions of pieces of content are shared on these services every day. Meta, *About Meta*, https://perma.cc/NLP2-W7MP. That likely means that Meta has to respond to several million pieces of content each year. In Q1 of 2024 alone, Meta "actioned" tens of millions of pieces of content classified as adult nudity and sexual activity, child endangerment, dangerous organizations and individuals, hate speech, and suicide and self-injury across Facebook and Instagram. Meta, *Community Standards Enforcement Report: Q1 2024 Report*, https://perma.cc/VCQ4-XSCS.

b. In Q1 of 2024, Google removed over 15 million channels and over 8 million videos from YouTube, the vast majority of which had fewer than ten views each at the time of removal due to the use of automated processes for reviewing and removing content that violated YouTube's terms of service. Google, *Google Transparency Report: YouTube Community Guidelines Enforcement*, https://perma.cc/YG36-EYKZ.

14. **Contextual Determinations.** The sheer number of content-moderation decisions that websites make each day can be matched by the degree of difficulty and nuance involved in the hardest judgment calls. Some content-moderation decisions are highly dependent on the context in which a post is shared, the language in which it is, and the cultural settings from which it comes and in which it is shared. Consequently, for many individual pieces of user-generated content, there will never be one "correct" content-moderation answer, and digital service providers will always struggle to deal with borderline cases as users push the boundaries of discourse online. As just one example, CCIA's covered members' content-moderation policies must account for the important distinction between purely objectionable and harmful content and content that is

educational, documentary, scientific, or artistic. So some of CCIA's covered members prohibit nudity on their websites but may allow nudity in an educational video of a medical professional conducting a physical examination. This requires websites to look at "multiple factors, including [] titles, descriptions[,] and context" to determine whether the content is truly objectionable and harmful. *E.g.*, Michael Grosack, *A Look at How We Treat Educational, Documentary, Scientific, and Artistic Content on YouTube*, YouTube Official Blog (Sept. 17, 2020), https://perma.cc/SEJ8-BTCX.

15. **Menu of Content-Moderation Actions.** Moderating objectionable and harmful content is not amenable to a one-size-fits-all approach. Some CCIA members are able to "age-gate" certain kinds of content, such that only adults can see it; other members cannot age-gate. Some CCIA members, if their user policies disclose it, might remove content or prevent whole classes of people from seeing it, while other CCIA members might take a different action. Through the use of warnings, disclaimers, labels, and providing additional context, CCIA members can inform their users what they deem important for the users to know. Further, some CCIA members also provide users the ability to further filter the content they see.

16. **Industry Collaboration with Child Safety Organizations and Law Enforcement.** To be sure, not all content-moderation decisions involve nuance. Certain illegal content like known CSAM can be addressed through the use of hash databases maintained by child safety organizations. By building complex automated tools overseen by global teams of human reviewers, digital services can remove known CSAM as soon as their services detect it. Additionally, CCIA members are at the forefront of combating CSAM online and contributing to hash-matching databases of online CSAM. *See* Google, *NCMEC, Google and Image Hashing Technology*, Google Safety Center, https://perma.cc/E3LZ-ZCZV.

17. **Bad Actors Innovate and New Forms of Objectionable and Harmful Content Arise.** CCIA members also face an uphill battle in combating objectionable and harmful content online as bad actors are constantly evolving in their attempts to bypass content moderation. Every time that CCIA's members develop new technological means to identify and moderate objectionable and harmful content, malicious actors attempt to find new ways to evade moderation. Thus, CCIA's members must constantly innovate. Additionally, new forms of objectionable and harmful content online threaten to arise all the time. For instance, the "Tide Pod Challenge" was a dangerous social media trend that required swift attention from CCIA's members. Due to the varied and unpredictable nature of this and other social media trends, CCIA members and other digital services modified their policies on self-harm and related topics to better protect user safety. This situation is not unique—once bad actors start noticing that websites are moderating particular content, they begin using creative misspellings or other tools like screenshots to share deleted content, emojis, and slang to evade further moderation efforts.

## V. Effect of Texas House Bill 18

18. Compliance with HB18 will be unduly burdensome and extremely costly for CCIA's covered members, causing them and their users irreparable harm. Specifically, the following provisions will require our members to spend large, unrecoverable sums to even attempt compliance—assuming compliance with all relevant provisions is possible:

a. HB18's requirements to create age-registration, age-challenge, and parental-verification procedures, Tex. Bus. & Com. Code §§ 509.051, 509.054, 509.101, may be cost- and resource-prohibitive for some members. These mandates all require large upfront investments to develop the necessary capabilities and ongoing expenditures (including of human resources) to maintain those capabilities. Specifically, the processes of confirming the age and identity of users,

confirming the age and identity of parents, and confirming the relationship between the user and the parent are inherently difficult and require capacities that many websites lack. Furthermore, in practice, these processes might require something akin to age-verification requirements, which are enormously difficult to maintain and deter users from creating accounts.

b. HB18's requirements for parental tools, *id.* §§ 509.054, 509.102, may be cost- and resource-prohibitive for some members. Like the provisions addressed above, these tools require large expenditures to develop and maintain. In turn, this expense may discourage websites from providing their services to minors.

19. HB18's monitoring and censorship requirements are also onerous for multiple reasons.

a. "[U]sing filtering technology" and "creating and maintaining a database of keywords used for filter evasion" *id.* § 509.053(b)(1)(B), (D), may be cost- and resource-prohibitive for some members. "Filtering" is not always the most appropriate strategy for effectuating site policies, and businesses use other moderation tools to most effectively address different categories of content. By mandating that websites must "filter" for all kinds of "harmful" content, HB18 compels websites to engage in activities that do not necessarily represent best practice for protecting users.

b. "[U]sing hash-sharing technology and other protocols," *id.* § 509.053(b)(1)(C), will be inordinately costly and burdensome because, while hash-sharing technology is an important tool used in certain contexts, (1) websites cannot possibly ex ante hash all content prohibited under the definitions of HB18, which are subjective and indefinite; (2) even if websites could do so, there is no existing mechanism to assess whether third parties' hashes represent an accurate interpretation of Texas law; (3) even if such a mechanism to enable reliance on third-party hashes

existed, websites have no way to compel others to agree to engage in such sharing; and (4) the infrastructure necessary to implement such a strategy would be extraordinary.

c. "[C]reating and maintaining a comprehensive list" of prohibited content and "making available to users a comprehensive description of the categories" of prohibited content, *id.* § 509.053(b)(1)(A), (F), are unfeasible requirements in light of the enormous amount of content uploaded to websites each day. The indefinite universe of content that HB18 prohibits cannot be listed in any "comprehensive" fashion, and even if such a list could be constructed, maintaining it would present an insurmountable task.

d. "[P]erforming standard human-performed monitoring reviews to ensure efficacy of filtering technology," *id.* § 509.053(b)(1)(E), cannot be reliably operationalized since there are no widely adopted "standards"—whether *de jure* or *de facto*—for human review of automated trust and safety filtering technology at this time. In any event, "filtering" does not accurately describe many trust and safety operations due to advances in machine learning technology, the limited contexts in which hashing and keyword filtering can be employed, and the finite nature of websites' resources.

e. "[M]aking available to users a comprehensive description of the categories of harmful material or other content described by Subsection (a) that will be filtered," *id.* § 509.053(b)(1)(F), requires websites to convey to users a virtually infinite and ever-growing set of online locations. First, as noted above, speaking comprehensively about all content falling within HB18, even as the universe of such content grows, is impossible. And even were it not continuing to grow, this indefinite set of content cannot be meaningfully and accurately described to everyday users in any understandable way.

f. "[M]aking available the digital service provider's algorithm code to independent security researchers," *id.* § 509.053(b)(1)(G), would require websites to disclose trade secrets and sensitive information that websites keep confidential to, among other things, protect users. Mandating such disclosure could put sensitive information in the hands of researchers located in or aligned with hostile foreign adversaries and other advanced persistent threats whose interests are antagonistic to user safety and/or U.S. national security. The fact that HB18 elsewhere states that "[n]othing in this subchapter may be construed to require a digital service provider to disclose a trade secret," *id.* § 509.058, does not resolve CCIA's concern, because that caveat does not reference the code-disclosure provision and cannot be read to necessarily nullify that provision.

20. Based on my years of experience and advocacy and my interactions with staff of digital service providers (including CCIA's members), I believe that HB18 will also impose enormous and prohibitive costs on smaller digital services that are not CCIA members. Those websites may be smaller as measured in users, volume of content, number of employees, or annual revenue—or all four. What will be difficult for CCIA members will be ruinous for many more websites across the Internet. Simply providing the various age-challenge processes and parental tools, *id.* §§ 509.051, 509.054, 509.101-03, may be cost- and resource-prohibitive for smaller websites. *See, e.g.*, Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), https://perma.cc/8RE8-PDVR. Because all websites must provide age-registration and age-challenge processes *regardless* of whether they allow minors, some websites could shut down entirely.

21. In addition, HB18's content-moderation requirements in Tex. Bus. & Com. Code § 509.053(b) may *weaken* CCIA's members' content-moderation systems. CCIA's members have adopted their own proprietary content-moderation systems designed for their unique communities

and adapted for the specific content-moderation challenges they face. An image-sharing service will likely require a different content moderation-approach than the one appropriate for microblogging services. HB18 will force companies to replace those well-tailored enforcement mechanisms with policies designed to comply with HB18—likely resulting in tools that might not be the most effective for moderating content. For example, increased use of filtering could result in over-inclusive moderation that would remove or restrict access to more speech than HB18's already-broad demands require.

22. Instead of top-down state mandates to filter speech in particular ways, CCIA members' private self-regulation and widely available parental controls are the more effective means to prevent children from encountering objectionable and harmful material. Specifically, parents have multiple means at their disposal including: (1) controlling the devices their children have access to and whether those devices can access the Internet; (2) imposing limitations on the websites those devices can access, using tools from both Internet service providers and device manufacturers; (3) limiting the amount of time minors can spend on those devices or those websites; and (4) using tools that the websites make available to parents precisely for these purposes.

* * *

23. If HB18 takes effect on September 1, 2024, CCIA's mission to promote open markets, open systems, and open networks would be directly, substantially, and irreparably harmed. Likewise, CCIA's covered members, as well as their users, will suffer irreparable harm.

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct to the best of my knowledge.

Executed on this 29th day of July, 2024, in Washington, D.C.

_____

Matthew Schruers